INTRODUCTION À LA CRYPTOGRAPHIE À BASE DES GROUPES DE CLASSES DE CERTAINS CORPS DE NOMBRES

ABDELMALEK AZIZI
ECOLE CIMPA "THÉORIE DES NOMBRES ET APPLICATIONS"
OUJDA 18-29 MAI 2015

1. Présentation

Le but de ce cours est de jeter un pont entre les formes quadratiques et la cryptographie elliptique.

Cet article est une introduction à la cryptographie utilisant les groupes de classes de certains corps de nombres et se basant sur le problème de la factorisation des grands nombres ou sur le problème du logarithme discret.

On va se contenter d'exposer les idées de base de certains travaux dans ce domaine en donnant un survol des résultats de théorie des nombres sur lesquels sont fondés ces travaux.

Plan :

(1) Généralités sur la cryptographie (RSA, Diffie-Hellman, ElGamal).

(2) Groupe de classes (ordres, idéaux réduits, groupe de classes, nombre de classes de certains ordres).

(3) Protocole de Buchmann-Williams sur les corps quadratiques imaginaires,

(4) Le Cryptosystème NICE.

2. Généralités

Dans cette section, on va donner quelques définitions utiles pour la suite.
Cryptographie : Art et science de l'étude des systèmes propres à résoudre les problèmes de confidentialité et d'authentification.
Cryptanalyse : Science permettant d'étudier les systèmes cryptographiques en vue de les tester ou de les casser.
Cryptologie : Science qui traite de la cryptographie et de la cryptanalyse.
Chiffrement d'un texte clair : transformation du texte clair en un texte incompréhensif ou illisible.
Déchiffrement : Opération inverse du chiffrement.

Il existe deux types d'algorithmes en cryptographie :
- *Algorithmes à clés secrètes* ou *crypto-systèmes symétriques* : Dans cette classe d'algorithmes on a une clé K1 pour chiffrer et une clé K2 pour déchiffrer ; K1 peut être calculé à partir de K2 et vice versa. On a souvent K1=K2 ; les clés K1 et K2 doivent être secrètes.
Exemples : DES, AES, etc.
- *Algorithmes à clé publique* ou *crypto-systèmes asymétriques* : Dans cette classe d'algorithmes on a deux clés, K1 et K2 ; K2 ne peut pas être calculé à partir de K1. La clé de chiffrement K1 peut être publique et la clé de déchiffrement K2 doit être secrète (clef privée).
Exemples : RSA, ElGamal, etc.
La sécurité des algorithmes repose en général sur certains problèmes difficiles à résoudre. En particulier, le problème de factoriser un grand nombre dans un temps convenable et le problème de calculer le logarithme discret d'un élément de certains groupe dans un temps convenable sont des problèmes difficiles et qui sont utilisés dans plusieurs algorithmes à clés publiques comme on va voir.

2.1. **RSA (Rivest, Shamir et Adleman 1978).** Chaque personne X possède une clé publique qui n'est rien d'autre que deux entiers n_X et s_X vérifiant les conditions suivantes :
(i) $n_X = pq$ où p et q sont des nombres premiers connus seulement de X et gardés secrets par X,
(ii) l'entier s_X est copremier avec l'entier $(p-1)(q-1)$ de sorte qu'il existe t_X tel que

$$1 \leq t_X < (p-1)(q-1) \text{ et } s_X t_X \equiv 1 \bmod (p-1)(q-1).$$

On publie la clé publique (s_X, n_X).
Chaque personne garde secrètement la clé privée (t_X, p, q).
Fonction de chiffrement : $E(M) = M^{s_X} = C \bmod n$.
Fonction de déchiffrement : $D(C) = C^{t_X} = M^{s_X t_X} = M \bmod n$.

2.2. **Logarithme discret.** Soient G un groupe cyclique fini dont la loi de composition est notée multiplicativement et g un générateur de G. Si l'ordre de G est égal à n et e est l'élément neutre de G ; alors $g^n = e$ et

$$G = \{e, g, g^2, g^3, ..., g^{n-1}\}.$$

Ainsi, pour tout élément h de G, il existe un entier naturel $m < n$ tel que $h = g^m$. L'entier m est appelé le logarithme discret de h relativement à la base g et on note alors

$$dlog_g(h) = m.$$

Il n'est pas facile en général de trouver le logarithme d'un élément quelconque de G. Cette difficulté de résoudre ce problème dans certains groupes G est utilisée en cryptographie pour chiffrer des messages.

Remarque 1. *Le groupe $G = (\mathbb{Z}/p\mathbb{Z})$ muni de la somme est un groupe où le problème du logarithme discret est facile à résoudre, tandis que le groupe $G = (\mathbb{Z}/p\mathbb{Z})^*$ muni de la multiplication est un groupe où le problème du logarithme discret est difficile à résoudre si le nombre premier p est très grand et est bien choisi.*

2.3. **Protocole de Diffie et Hellman.** Deux personnes veulent s'échanger une clé ; ils se mettent d'accord sur un groupe cyclique G, un générateur g de G et n l'ordre de G.
Alice choisit un grand nombre entier x inférieur à n et envoie à Bachir le résultat du calcul : $A = g^x$.
Bachir choisit un grand nombre entier y inférieur à n et envoie à Alice le résultat du calcul : $B = g^y$.
Alice calcule $k = B^x$;
Bachir calcule $k' = A^y$;
Les valeurs k et k' sont toutes deux égales à g^{xy} qui est la clé échangée entre les deux personnes.
Si g, A, et B sont connus ; trouver k est un problème appelé problème de Diffie-Hellman.

2.4. **Cryptosystème d'ElGamal.** Le système de cryptage d'ElGamal est un exemple de cryptage en liaison avec l'échange de clè de Diffie-Hellman défini sur le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $p-1$. La sécurité de ce système de cryptage est basée sur la difficulté de résoudre le problème de Diffie-Hellman dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

Si Alice veut envoyer un message m à Bachir, elle calcule $c = g^{xy}m$ et envoie (X, c) à Bachir. Pour décrypter ce message, Bachir doit tout simplement multipler par l'inverse de la clé dans le groupe G :

$$g^{p-1-xy}c = g^{p-1-xy}g^{xy}m = m.$$

Remarques 1. *(1) Tout ce qui précède reste vrai pour un groupe cyclique fini G quelconque. La sécurité de ce système de cryptage est basée sur la difficulté de résoudre le problème de Diffie-Hellman.*

(2) Il est clair que casser le protocole d'échange de clés de Diffie-Hellman c'est casser le cryptosystème d'ElGamal. Inversement, si on sait casser le cryptosystème d'ElGamal, c'est qu'on sait déchiffrer tout message chiffré par la méthode d'ElGamal. En particulier, si le message chiffré est $c = 1$, alors de l'égalité $1 = g^{xy}m$, on déduit que la clé est $g^{xy} = m^{-1}$.

(3) Pour le cryptosystème d'ElGamal dans le cas d'un groupe cyclique quelconque on représente un message m par un élément g_m du groupe et le message chiffré est $c = Kg_m$. Une question qui se pose c'est comment représenter le message m par l'élément g_m.

3. Idéaux et groupe de classes d'un ordre quadratique

Soit $\mathbb{L} = \mathbb{Q}(\sqrt{\Delta})$ un corps de nombres quadratique avec Δ un entier congru à 0 ou à 1 modulo 4. Soit $O_{\mathbb{L}}$ l'anneau des entiers de $\mathbb{L}$; on appelle *ordre quadratique de discriminant* Δ tout $\mathbb{Z}$-module de rang 2 contenant 1 et engendré par une base de $\mathbb{L}/\mathbb{Q}$.

On montre que tout ordre quadratique est de la forme $O_\Delta = \mathbb{Z}+\mathbb{Z}(\Delta+\sqrt{\Delta})/2$. Le discriminant Δ est dit fondamental si Δ ou $\Delta/4$ est sans facteur carré ; dans

ce cas l'ordre quadratique est dit *ordre maximal*; on note son discriminant par Δ_1.
Tout autre discriminant Δ est de la forme $f^2\Delta_1 = \Delta_f$ pour un certain entier positif f appelé le conducteur de l'ordre quadratique. Soit Δ_1 la partie sans facteur carré de Δ ; alors l'anneau $O_{\mathbb{L}} = O_{\Delta_1}$ est égal à $\mathbb{Z} + \mathbb{Z}\omega$ avec

$$\omega = \begin{cases} \sqrt{\Delta_1} & \text{si } \Delta_1 \equiv 2,3 \text{ modmod4}, \\ \frac{(1+\sqrt{\Delta_1})}{2} & \text{si } \Delta_1 \equiv 1 \text{ modmod4}. \end{cases}$$

Le théorème suivant décrit explicitement les idéaux de O_{Δ_f}.

Théorème 1. *(voir* [13]*)*
Tous les idéaux entiers de O_{Δ_f} sont de la forme suivante

$$I = d \times \left(\mathbb{Z}a + \mathbb{Z}\frac{b+\sqrt{\Delta_f}}{2} \right),$$

avec $a, b, d \in \mathbb{Z}; 4a \mid b^2 - \Delta_f$ et $N_{\mathbb{L}/\mathbb{Q}}(I) = |O_{\Delta_f}/I| = (d^2a)$.
Inversement, tout $\mathbb{Z}$-module de cette forme est un idéal entier de O_{Δ_f}.
Un idéal fractionnaire de O_{Δ_f} est de la forme αI où I est un idéal entier et $\alpha \in \mathbb{Q}$.

Remarque 2. *On a $O_{\Delta_f} \subset O_{\Delta_1}$ et $[O_{\Delta_1} : O_{\Delta_f}] = f$.*
Si I est un idéal de O_{Δ_f} alors IO_{Δ_1} est un idéal de O_{Δ_1}.
Inversement, si I est un idéal de O_{Δ_1} alors $I \cap O_{\Delta_f}$ est un idéal de O_{Δ_f}.
Soit $I(O_{\Delta_1}, f)$ (respectivement $I(O_{\Delta_f}, f)$) l'ensemble des idéaux de O_{Δ_1} (respectivement O_{Δ_f}) premiers avec f.
On a les deux correspondances bijectives suivantes :

$$\begin{cases} \phi : I(O_{\Delta_1}, f) & \longrightarrow I(O_{\Delta_f}, f) \\ I & \longmapsto \phi(I) = I \cap O_{\Delta_f} \end{cases}$$

$$\begin{cases} \phi^{-1} : I(O_{\Delta_f}, f) & \longrightarrow I(O_{\Delta_1}, f) \\ I & \longmapsto \phi^{-1}(I) = IO_{\Delta_1, f} \end{cases}$$

Grace aux résultats du Théorème 1, on peut choisir a positif et a, b et $c = (b^2 - \Delta)/4a$ premiers entre eux. Ainsi un idéal I est représenté par (d, a, b).

Quand $d = 1$ dans le théorème précédent, l'idéal est dit **primitif** et on pose $I = (a, b)$ et on a $N(I) = a$.

Définition 2. *Un idéal primitif $I = (a, b)$ est dit réduit si et seulement si il n'existe aucun $\alpha \in I$ tel que $\mid \alpha \mid < a$ et $\mid \overline{\alpha} \mid < a$. En particulier si $\Delta_f < 0$, un idéal primitif $I = (a, b)$ est réduit si et seulement si :*
(1) $a \leq c = (b^2 - \Delta_f)/4a$,
(2) $-a \leq b \leq a$,
(3) Si $a = c$, alors $b > 0$.

Deux idéaux I_1 et I_2 sont équivalents si et seulement si il existe $\alpha,\ \beta \in O_{\Delta_f}$ tel que $I_1(\alpha) = I_2'(\beta)$.
Un idéal fractionnaire I est inversible si et seulement si il existe un idéal fractionnaire J tel que $IJ = O_{\Delta_f}$.

Soit $P_{\Delta_f,f}$ l'ensemble des idéaux principaux premiers avec f ; alors $I(O_{\Delta_f}, f)/P_{\Delta_f,f}$ est un groupe qu'on note par $Cl(O_{\Delta_f})$.
L'ordre du groupe $Cl(O_{\Delta_f})$ noté par $h(\Delta_f)$ est appelé le nombre de classes de O_{Δ_f}.

Théorème 3. *Le nombre de classes $h(\Delta_f)$ est un multiple de $h(\Delta_1)$; en particulier si $f = q$ est un nombre premier alors on a*

$$h(\Delta_f) = h(\Delta_1)(q - \left(\frac{\Delta_1}{q}\right)) \text{ si } \Delta_1 < -4;$$
$$h(\Delta_f) = h(\Delta_1)(q - \left(\frac{\Delta_1}{q}\right))\frac{R_{\Delta_1}}{R_{\Delta_q}} \text{ si } \Delta_1 > 0;$$

où R_{Δ_f} est le régulateur de l'ordre O_{Δ_f}.
Dans le cas réel on a $\epsilon_{\Delta_q} = \epsilon_{\Delta_1}^t$ pour un entier $t > 0$. De plus, on a $R_{\Delta_f} = log(\epsilon_{\Delta_f})$ et par suite $t = R_{\Delta_q}/R_{\Delta_1}$ avec t divisant $(q - \left(\frac{\Delta_1}{q}\right))$.

De plus, on a :

Théorème 4. *Chaque classe d'équivalence de $Cl(O_{\Delta_f})$ contient un idéal réduit. Si $\Delta_f < 0$ il existe un unique idéal réduit dans chaque classe ; Si $\Delta_f > 0$ il en existe plusieurs. De plus, on a :*
(1) Si I est un O_{Δ_f}-idéal primitif tel que $N(I) < \sqrt{|\Delta_f|}/2$, alors I est un idéal réduit.
(2) Si I est un O_{Δ_f}-idéal réduit, alors $N(I) < \sqrt{\Delta_f}$ si $\mathbb{L}$ est réel et $N(I) < \sqrt{\Delta_f/3}$ si $\mathbb{L}$ est imaginaire.

Remarque 3. *Soient $I = (a, b)$, $\bar{a}$ le nombre premier le plus proche de a et $\bar{b}$ le nombre premier le plus proche de b. On pose $\bar{I} = (\bar{a}, \bar{b})$ et $d = a - \bar{a}$ est la distance entre I et $\bar{I}$. Dans le cas réel chaque classe contient un nombre fini d'idéaux réduits (formant un cycle) ; on peut définir un unique représentant qui est minimal dans le sens suivant :*
Un idéal réduit $I = (a', b')$ est minimal dans son cycle si et seulement si $\forall \bar{I} = (\bar{a}, \bar{b}) \sim I = (a', b')$ on a $a' < \bar{a}$ ou bien $\bar{a} = a'$ et $b' < \bar{b}$.

La relation entre le groupe des classes des formes quadratiques définies positives $Cl(\Delta)$ et $Cl(O_\Delta)$ est donnée dans le théorème suivant (voir [8]).

Théorème 5. *L'application qui envoie la classe d'équivalence de la forme quadratique binaire $f(x, y) = ax^2 + bxy + cy^2$ de discriminant $\Delta = b^2 - 4ac$ vers la classe de l'idéal $I_f = \mathbb{Z}a + \mathbb{Z}\frac{b+\sqrt{\Delta}}{2}$ est une bijection entre $Cl(\Delta)$ et $Cl(O_\Delta)$.*

Grâce à ce théorème, on peut identifier les classes des idéaux dans $Cl(O_\Delta)$ et les classes des formes quadratiques binaires de discriminant Δ. Ainsi l'étude de plusieurs questions sur le groupe de classes se transforme en une étude du même

genre sur le groupe des classes des formes quadratiques comme la question de réduction des idéaux qui se transforme en une question de réduction des formes quadratiques.

4. Cryptographie via le groupe de classes

Fonction à sens unique

Une fonction à sens unique est une fonction facile à calculer mais dont l'inverse est difficile à calculer (même de façon probabiliste).
Par exemple, le logarithme discret : $f(x) = g^x \bmod n$ est une fonction à sens unique.
De plus, certaines fonctions à sens unique peuvent être construites à partir du problème de la factorisation de grands entiers (ex. RSA : $f(x) = x^s \bmod n$ où (s, n) est une clé publique de RSA).

Fonction de hachage

Pour contourner le problème de la longueur des clés on utilise plutôt une empreinte digitale obtenue à l'aide d'une fonction de hachage h qui transforme des phrases longues en des phrases courtes de taille fixe. En particulier, une bonne fonction de hachage est une fonction satisfaisant les propriétés suivantes :
Étant donné M, il est facile de calculer $h(M)$.
Étant donné $h(M)$, il est difficile de calculer M.
Étant donné M, il est difficile de trouver un autre message M' tel que $h(M) = h(M')$.
Il est souvent utile d'avoir la propriété suivante :
Il est difficile de trouver deux messages aléatoires M et M' tels que $h(M) = h(M')$.
Exemple.
Soient p un nombre premier impair très grand tel que $q = \frac{p-1}{2}$ est aussi un nombre premier, α et β deux générateurs du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Soit h la fonction de $\{0, 1, ..., q-1\}^2$ vers $(\mathbb{Z}/p\mathbb{Z})^*$ telle que $h(x, y) = \alpha^x \beta^y \bmod p$; alors h est une fonction de hachage telle que si la dernière propriété, dite collision, se produit, alors le logarithme discret de β dans la base α est facile à trouver.

Caractéristiques des bons groupes de classes à utiliser :

Dans tous les cryptosystèmes qu'on va évoquer, on va utiliser un groupe de classes ou l'un de ses sous-groupes cycliques qu'on va noter par G. L'ordre de G est n et g est l'un de ses générateurs. Un groupe G où les cryptostèmes seront efficaces doit satisfaire les conditions suivantes :
(1) Le discriminant doit être choisi de telle sorte que le problème du logarithme discret ou le problème de factorisation soit un problème difficile à résoudre.
(2) Le discriminant et l'ordre $n = h(\Delta)$ doivent être très grands pour éviter certaines attaques.
(3) Le calcul arithmétique dans G doit être faisable dans un temps acceptable (calcul de chiffrement et de déchiffrement).

4.1. **Protocole de Buchmann-Williams d'échange de clés.** Pour tout idéal I primitif, nous allons noter par I_{red} son idéal réduit. Nous rappelons que I_{red} est

équivalent à I.
Nous pouvons maintenant décrire le protocole de Buchmann-Williams :
Soient deux utilisateurs Alice et Bachir qui vont choisir un entier $\Delta < 0$ tel que $\mid \Delta \mid$ est discriminant fondamental très grand, et un idéal I de $O_{\mathbb{L}}$. Les valeurs de Δ et de l'idéal I vont être publiques.

(1) Alice choisit un entier x et elle calcule l'idéal réduit J tel que $J \sim I^x$. Elle envoie J à Bachir.

(2) Bachir choisit un entier y et calcule l'idéal réduit L tel que $L \sim I^y$. Il envoie L à Alice.

(3) Alice calcule l'idéal réduit $(L^x)_{red}$ équivalent à L^x ; Bachir calcule l'idéal réduit $(J^y)_{red}$ équivalent à J^y.

Comme $L^x \sim J^y \sim I^{xy}$, l'idéal réduit calculé par Alice et Bachir est le même et donc on trouve $(L^x)_{red} = (J^y)_{red}$. Alice et Bachir peuvent prendre comme clé secrète $(L^x)_{red} = (J^y)_{red}$.
Un discriminant admissible pour cet échange est le suivant : $\Delta = -p_1p_2$ où p_1 et p_2 sont deux premiers tels que $p_1p_2 \equiv 1 \bmod 4$ et le symbole de Legendre $(\frac{p_1}{p_2})$ est égal à -1.

La sécurité de ce protocole est basée sur la difficulté de résoudre le problème du logarithme discret dans le groupe de classes des corps de nombres quadratiques imaginaires. La difficulté de résoudre le problème du logarithme discret est de même niveau que la difficulté de calculer le nombre de classes des corps quadratiques imaginaires (voir [11] pour plus de détails).
Les algorithmes utilisés pour résoudre le problème du logarithme discret sont en général exponentiels, et sont sous-exponentiels sous l'hypothèse de Riemann généralisée. Ce qui rend le protocole de Buchmann-Williams tout à fait sûr (vour [11], [1] et [2] pour plus de détails sur la sécurité de ce protocole). En utilisant le concept de distance entre idéaux de Shanks [15], Buchmann et Williams [5, 2] ont pu définir un protocole d'échange de clés sur les corps quadratiques réels.

4.2. **Utilisation du Cryptosystème d'ElGamal.** Une personne A choisit un discriminant Δ suivant le niveau de sécurité qu'elle veut. Elle choisit ensuite un idéal I et un entier $x < n$ où n est l'ordre du groupe de classes. Elle calcule l'idéal J qui est le réduit de l'idéal I^x et elle publie (Δ, I, J).
Une personne B veut envoyer un message m à A. Pour en crypter le message m, elle choisit un entier $y < n$ et calcule l'idéal réduit L de I^y. Ensuite elle calcule l'idéal réduit de J^y qu'on note par K. Le texte chiffré est alors $C = (L, c)$ où $c = m \oplus f(K)$, f est une fonction de hachage et $\oplus$ est l'opération xor.
Pour décrypter, la personne B calcule $K = J^y$ et retrouve le message $m = c \oplus f(K)$.
Si $K = (a, b)$, Buchmann et Williams dans[4] ont utilisé $f(K) = a$ où $a = N(K)$ la norme de l'idéal K.

Remarque 4. *(1) Le protocole d'échange de clés de Diffie-Hellman a été défini par Buchmann et Williams sur les corps quadratiques réels ; non pas sur un groupe*

mais sur un ensemble d'idéaux fractionnaires réduits (voir [5]*).*

(2) Soit p le plus grand nombre premier inférieur à $\frac{\sqrt{|\Delta|}}{2}$. On peut injecter un message $m < p$ dans l'idéal $M = (m, b)$ où $b^2 \equiv \Delta \bmod 4m$. Cet idéal peut être utilisé dans le cryptosystème d'ElGamal comme dans le cas général d'un groupe cyclique. Soit $D = N^2 + 1$ et $\mathbb{L} = \mathbb{Q}(\sqrt{D})$ c'est un corps appelé corps de Degert ; le calcul de l'idéal minimal réduit se fait efficacement et par suite le cryptosystème d'ElGamal sur le groupe de classes de ce dernier corps quadratique réel sera efficace (pour plus de détails voir [14]*).*

5. Le Cryptosystème NICE (New Ideal Coset Encryption)

On reprend les deux correspondances suivantes :

$$\begin{cases} \phi : I(O_{\Delta_1}, f) & \longrightarrow I(O_{\Delta_f}, f) \\ I & \longmapsto \phi(I) = I \cap O_{\Delta_f} \end{cases}$$

$$\begin{cases} \phi^{-1} : I(O_{\Delta_f}, f) & \longrightarrow I(O_{\Delta_1}, f) \\ I & \longmapsto \phi^{-1}(I) = IO_{\Delta_1, f} \end{cases}$$

Ces deux bijections vérifient les propriétés suivantes :

(1) Elles sont compatibles avec la multiplication des idéaux.

(2) Elles laissent fixe le coefficient a de chaque idéal ($I = (a, b)$).

(3) ϕ préserve la réduction mais ϕ^{-1} ne la préserve pas.

(4) ϕ et ϕ^{-1} se calculent efficacement si le conducteur f est connu.

(5) ϕ et ϕ^{-1} sont incalculables si le conducteur f n'est pas connu.

Sur ces dernières propriétés se base le cryptosystème NICE (New Ideal Coset Encryption) suivant :
Clé privée : grands nombres premiers p et q où $p \equiv 3 \bmod 4$ formant $\Delta_1 = -p$ et $\Delta_q = -pq^2$,
Clé publique : $(\Delta_q, k, n, \mathbf{p})$ où
k est la longueur des bits de $\sqrt{\Delta_1}/4$,
n est la longueur des bits de $(q - (\frac{\Delta_1}{q}))$,
$\mathbf{p}$ est un O_{Δ_q}-idéal tel que $\phi^{-1}(\mathbf{p})$ est principal.
Si m est le texte clair, on pose

$$\bar{m} = m \underbrace{000...000}_{t \text{ zeros}}.$$

Pour en crypter $\bar{m}$ avec la clé $(\Delta_q, k, n, \mathbf{p})$, on suit les étapes suivantes :

(1) chercher le plus petit nombre premier $l > \bar{m}$ tel que Δ_q soit un carré modulo l ;

(2) résoudre $b^2 \equiv \Delta_q \bmod 4l$ et poser $\mathbf{m} = (l, b)$;

(3) générer un nombre aléatoire $r \in \{1, 2, ..., 2^{n-1}\}$;

(4) le texte chiffré est alors l'idéal réduit

$$c = \rho_{\Delta_q}(\mathbf{m}\mathbf{p}^r).$$

Pour décrypter c avec la clé privée (p, q) :

(1) Calculer $\mathbf{M} = \rho_{\Delta_1}(\phi^{-1}(c)) \sim \phi^{-1}(c) \sim \phi^{-1}(\mathbf{m})$;

(2) m est alors les $k - t$ premiers bits de $N(\mathbf{M})$.

Remarque 5. *1. L'entier t est choisi très grand pour que le déchiffrement soit facile et aussi pour éviter certaines attaques.*
2. Il existe une cryptanalyse réussie du cryptosystème NICE (voir [6] *et* [7]*).*
3. Il y a une adaptation de ce cryptosystème aux corps quadratiques réels : avec les mêmes notations et données et un changements au niveau de p et de $\bar{m}$: le premier $p \equiv 1 \bmod 4$, $\Delta_1 = p$ et $\Delta_q = pq^2$ et le

$$\bar{m} = \underbrace{100...000}_{u\text{-}1zeros}\, m\, \underbrace{000...000}_{t\ zeros}.$$

où u est choisi assez grand de tel sorte que la probabilité que chaque O_{Δ_1}-classe d'idéaux contienne au plus un idéal réduit dont la norme est égale à $100...000X$ (pour plus de détails voir [12]*) soit élevée.*
4. Pour une bonne sécurité, R_{Δ_q} doit être choisi grand pour assurer un grand nombre d'idéaux réduits dans une classe ; ce qui va rendre très difficile une recherche exhaustive dans un cycle d'idéaux réduits. Tandis que R_{Δ_1} doit être assez petit pour assurer un nombre petit d'idéaux réduits dans une classe ; ce qui va rendre efficace toute recherche exhaustive dans un cycle d'idéaux réduits (pour plus de détails voir [12]*).*

6. Conclusions

Plusieurs généralisations des cryptosystèmes présentés dans les paragraphes précédents avaient été établies dans certains cas de corps de nombres (corps biquadratiques cycliques imaginaires, corps cubiques cycliques, corps purs de degré 4, corps de Stender, ...). Actuellement, la recherche dans ces domaines est moins active qu'avant, mais elle existe encore. Plusieurs chercheurs qui ont lancé la recherche dans cet axe ont bifurqué vers d'autres directions de recherches ; peut être qu'ils sont convaincus que c'est un axe sans issue ou bien leurs idées dans cette direction axe sont stériles ; mais ce qui est sûr c'est que pour lancer la recherche dans cet axe il faut de nouvelles idées et des corps bien spéciaux.

D'un autre côté, même si la cryptographie sur les groupes de classes des corps de nombres n'a pas eu un succès remarquable par rapport à la cryptographie elliptique, elle développe dans sa partie théorique une bonne partie de la théorie algébrique des nombres.
Les cryptosystèmes qu'on a décrits reposent sur la difficulté de factoriser un grand nombre ou bien sur la difficulté de résoudre le problème du logarithme discret ; cependant, si l'ordinateur quantique voit le jour les deux problèmes précédents deviennent des problèmes faciles à résoudre ; ce qui va pousser les chercheurs à utiliser d'autres idées et techniques pour neutraliser la puissance de calcul de l'ordinateur quantique.

Références

[1] J. F. Biasse, M. J. Jacobson Jr, A. K. Silvester, *Security Estimates for Quadratic Field Based Cryptosystems*, Information Security and Privacy, 15th Australasian Conference, ACISP 2010, Sydney, Australia, LNCS.

[2] J. A. Buchmann et U. Vollmer, *Binary quadratic forms, an algorithmic approach*, Springer-Verlag, Heidelberg, 2007.

[3] J. A. Buchmann, R. Scheidler et H. C. Williams, *Implementation of a key exchange protocol using real quadratic fields, extended abstract*, Advances in Cryptology, Heidelberg EUROCRYPT '90', LNCS 473, 1991, 98–109.

[4] J. A. Buchmann et H. C. Williams, A Key-Exchange System Based on Imaginary Quadratic Fields, *J. Cryptology* **1** (1988), 107–118.

[5] J. A. Buchmann and H. C. Williams, *A key exchange system based on real quadratic fields Extended abstract*, CRYPTO '89 Proceedings on Advances in cryptology, 335–343.

[6] G. Castagnos, F. Laguillaumie, *On the security of Cryptosystems with Quadratic Decryption : The Nicest Cryptanalysis*, 28 th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Dec 2009, Tokyo Japan. Lecture Notes in Computer Science, pp. 260-277.

[7] G. Castagnos, A. Joux, Fabien Laguillaumie, Phong Q. Nguyen, *Factoring pq^2 with Quadratic Forms : Nice Cryptanalyses.* Springer Berlin Heidelberg. ASIACRYPT'2009 - 15th Annual International Conference on the Theory and Application of Cryptology and Information Security, A, Dec 2009, Tokyo, Japan. pp.469-486, Lecture Notes in Computer Science.

[8] D. A. Cox, *Primes Of The Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley and Sons, Inc, 1989.

[9] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory* **31** (1985), 469-672.

[10] G. Frey, T. Lange, *Mathematical Backgound of Public Key Cryptography.* Séminaires et Congrès, 11, SMF 2005, pp. 41-73

[11] S. Hamdy and B. Möller, *Security of Cryptosystems Based on Class Groups of Imaginary Quadratic Orders*, Advan in Crypto, ASIACRYPT, 2000, LNCS.

[12] M. J. Jacobson Jr., R. Scheidler, and D. Weimer, *An Adaptation of Nice Cryptosystem to Real Quadratic Orders*, Progress in Cryptologie, AFRCACRYPT, Springer 2008, pp. 191-208.

[13] H. W. Lenstra, *On The Calculation Of Regulators and Class Numbers of Quadratic Fields*, Journées Arithmétiques 1980, Cambridge University Press, 1982.

[14] Daniel Schielzeth and Michael E. Pohst, *On Real Quadratic Number Fields Suitable for Cryptography.* Experimental Mathematics, 14 :2 (2005), page 185.

[15] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proc. 1972 Number Theory Conf., Boulder, Colorado, 1973, 217–224.

Département de Mathématiques et Informatique, Faculté des Sciences, Université Mohamed 1, Oujda, Maroc.

E-mail address: abdelmalekazizi@yahoo.fr